简译版

不断增长但可预防的移动威胁——中间人攻击

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Man-in-the-Middle Attacks: A Growing but Preventable Mobile Threat		
原文作者	汤姆·托瓦（Tom Tovar）	**原文发布日期**	2020年4月15日
作者简介	汤姆·托瓦是移动解决方案平台Appdome的首席执行官兼创始人。		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/man-in-the-middle-attacks-a-growing-but-preventable-mobile-threat/a/d-id/1337515		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

不断增长但可预防的移动威胁——中间人攻击

汤姆·托瓦

2020 年 4 月 15 日

多年来，中间人（MitM）攻击一直备受关注，使用该技术的黑客变得更加老练，他们越来越多地以移动设备为目标。

MitM 攻击的要点很简单。网络犯罪分子拦截了移动用户与该用户试图访问的服务器之间的通信。攻击者可以采取两种模式：主动模式或被动模式。他们可以被动地监视通信，窃取密码和其他敏感数据。他们还可以主动更改信息，甚至可以将恶意代码注入到用户认为安全的会话中。

MitM 攻击最常见的方式之一是模仿合法热点的仿冒 Wi-Fi 接入点，攻击者能够查看和控制通过它们的所有流量。

但是还有许多其他更隐蔽的手段，例如 SSL“剥离”。在这种情况下，当用户发出 HTTP 请求启动安全的 HTTPS 会话时，攻击者将拦截此请求，而是与其自身建立安全连接，并与受害者建立不安全的连接。然后，攻击者就充当了他们之间的桥梁，能够以明文形式查看来自受害者的所有信息。

有多种方法可以抵御 MitM 攻击。例如，移动应用程序开发人员和企业可以在应用程序上添加安全功能，以使 MitM 攻击从根本上变得不可能。不幸的是，由于（企业和开发人员）缺乏安全技能，或是承受着无法在交付期限内完成任务的压力，这些安全功能常常没有内置到应用程序中。正如《Verizon 移动安全性指数 2020 报告》指出的那样，有 43％的组织机构在构建移动安全性时有意地偷工减料，只为快速交付工作。

随着移动设备在瞬息万变的世界中继续占有一席之地，移动应用程序开发人员为 MitM 攻击提供新级别的保护至关重要。首先，开发人员需要意识到不同级别的 MitM 攻击所需的检测和保护级别不同。在最基本的检测级别上，有一些工具可以验证证书的真伪。一旦工具检测到证书是伪造的，连接将会被断开。

但是，要防御更复杂的 MitM 攻击，也就需要我们采取高加先进的检测和保护措施。对于移动应用程序，构建应用程序时应包含以下两个最重要的保护措施：

采取 TLS（传输层安全）密码套件和安全版本协议：密码套件是一组用于保护 TLS 连接的算法。可以使用的密码套件有数百种，它们提供的安全级别差别很大。有些非常不安全。建立应用程序将接受的密码很重要，以确保仅允许使用获准的、安全的密码套件。

同样，较旧的 TLS 版本容易受到已知的网络攻击。因此，将网络连接的 SSL/TLS 版本限制为仅允许的安全版本非常重要。

强制执行证书角色：除非证书包含强制执行的角色，否则来自恶意行为者的证书会欺骗移动设备，使其认为连接是可信的。方式如下：在信任链上，“较高级别”证书可以验证“较低级别”证书的真实性。最终，信任链建立在提供者颁发的证书上，运行应用程序的平台则信任该提供者。

服务器提供给最终用户的证书称为“叶”证书；但是，无论证书的角色如何，证书之间都没有功能上的区别。因此，虽然“叶”证书不能算是证书颁发机构，但是每个证书都可以用给另一个证书签名。结果，恶意行为者可以获得他们自己的证书，这将允许他们能够发起 MitM 攻击。

例如，一个正常的证书链链可能是这样的：

您的浏览器/Android 系统/iPhone 信任“Go Daddy 根证书颁发机构- G2”，“Go Daddy 根证书颁发机构- G2”签名了“Go DaddySecure 证书颁发机构- G2”，而“Go DaddySecure 证书认证机构- G2”又为您的公司域名进行了签名，所以您的浏览器/Android/iPhone 就会信任您的公司域名，并与之建立安全的连接。

但是，如果恶意行为者获得了自己的证书，则他们可以拦截通过此证书链进行的通信：

您的浏览器/Android 系统/iPhone 信任“Go Daddy 根证书颁发机构- G2”，“Go Daddy 根证书颁发机构- G2”签名了“Go DaddySecure 证书颁发机构- G2”，此时就会出现中间人--恶意域名网址，它会凭借自身的自签名证书，伪装成您的公司域名，从而“Go DaddySecure 证书颁发机构- G2”会为其签名认证；然后再伪装成“Go DaddySecure 证书颁发机构- G2”为您的公司域名签名认证。这样，您的浏览器/Android/iPhone 同样会以为此证书链的一切正常，建立起不安全连接。

为了阻止这种攻击，每个证书都必须在“基本约束”通用扩展中包含有关其角色的信息。但是，如果证书没有此扩展，则 TLS 实现不会强制执行该扩展。

执行基本约束扩展的存在和证书在链中的角色是至关重要的。通过强制执行每个证书和网络连接的角色，可以维护信任链以防止 MitM 攻击。

这些基本措施为防范 MitM 攻击奠定了基础，不仅保护了移动终端用户，也保护了应用开发商的声誉。为了加速交付而忽略移动安全性可能很容易，但是一旦发生违规，应用开发商想要重新获得声誉和弥补损失是非常困难的。

借助于先进的 MitM 防御技术和其他安全功能，为了更有效地防范 MitM 攻击，最好先确保应用程序的安全。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）
安天企业安全公司更多信息请访问： http://www.antiy.cn
安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com